IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Brian Showers et al.
Title:	DISTRIBUTED SECRETS FOR VALIDATION OF GAMING TRANSACTIONS

Application No.:	09/740,325	Filed:	December 18, 2000
Examiner:	Mark Alan Sager	Group Art Unit:	3714
Atty. Docket No.:	027-0002	Confirmation No.:	4574

April 4, 2005

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed on December 2, 2004. A Two Month Extension of Time is being submitted herewith to extend the time for filing this Appeal Brief to April 2, 2005. Since April 2, 2005 is a Saturday, the time for filing the Appeal Brief is extended to Monday, April 4, 2005. The fee required under 37 C.F.R. § 41.20(b)(2) is provided in the accompanying Transmittal.

REAL PARTY IN INTEREST

The real party in interest in this appeal is Trilogy Development Group, Inc., the assignee of record.

RELATED APPEALS AND INTERFERENCES

There are no known prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-38 are pending and stand rejected. Rejected claims 1-38 are the subject of this appeal.

STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

A concise explanation of the subject matter defined in each of the independent claims involved in the appeal is set forth below. Each means plus function claim is identified below and the structure, material, or acts described in the specification as corresponding to each claimed function is set forth below.

Claim 1 is directed to a method for executing nested first- and second-type commit reveal sequences, wherein the first-type commit/reveal sequence commits an outcome generator to a set of outcomes. The first-type commit/reveal sequence is described, e.g., on page 7, line 28-page 8, line 4 (paragraph 1026) and illustrated in Fig. 3. The commit portion of the commit/reveal sequence occurs when game server 310 encrypts, e.g., order of a deck of cards, and supplies an encoding 351 to players 320. The encoding commits the game server to a particular outcome, e.g., the order of the deck of cards. The first and second-type commit reveal sequences are nested such that the second-type commit reveal sequence is nested within the first.

The second-type commit/reveal sequence commits at least each player to a respective index contribution and only thereafter does each player reveal the respective index contributions. As described, e.g., on page 8, lines 5-19 (paragraphs 1027 and 1028), game server 310 utilizes index contributions from the players (such as a random number) to generate the index of a card in the deck to deal. Each player commits to its index contribution prior to revealing the contribution and without knowledge of other player's contribution. As described on page 9, lines 6-13 (paragraph 1030), when each player has obtained the transformationally secured version of the index contribution of every other player ("SECURED X_i's in Fig. 3), the players then exchange the underlying index contributions (354 in Fig. 3). As described on page 9, lines 14-

19, paragraph 1031, contributions of the various players are combined to compute a selector into the committed deck.

Finally the set of outcomes is revealed for validation. As described, e.g., on page 10, lines 17-28 (paragraph 1034), the game server 310 reveals contents of deck 361, which each of the players may verify against the committed deck 362.

Claim 11 is directed to a verifiable gaming transactions method that transformationally secures an encoding of a predetermined set of outcomes and supplies one or more players with the transformationally secured encoding. As described on page 7, line 28-page 8, line 4 (paragraph 1026) and illustrated in Fig. 3, server 310 encrypts, e.g., a deck of cards and supplies an encoding 351 to players 320. Claim 11 further recites receiving a transformationally secured player index from each of the one or more players; and selecting a particular one of the outcomes for revealing to the one or more players based on a combination of the player indices. As described, e.g., on page 8, lines 5-19, paragraphs 1027 and 1028, game server 310 utilizes index contributions from the players to generate the index of a card in the deck to deal. Each player commits to its index contribution prior to revealing the contribution and without knowledge of other player's contribution. As described on page 9, lines 6-13, paragraph 1030, when each player has obtained the transformationally secured version of the index contribution of every other player, the players then exchange the underlying index contributions (see 354 in Fig. 3). As described, e.g., on page 9, lines 14-19, paragraph 1031, contributions of the various players are combined to compute a selector into the committed deck.

Claim 20 is directed to a verifiable gaming transactions method. The method includes receiving a transformationally secured encoding of a predetermined set of outcomes for a gaming transaction. See, e.g., Fig. 3, element 351 and page 7, line 28 to page 8, line 4 (paragraph 1026). Claim 20 further recites supplying a transformationally secured encoding of a player input (Fig. 3, 352) and after each of zero or more other participants in the gaming transaction has supplied a transformationally secured corresponding input, supplying the player input (Fig. 3, 354). As described in paragraph 1030, when each player has obtained the transformationally secured version of the index contribution of every other player , the players then exchange (354) the underlying index contributions. The claim further recites accessing a particular one of the

outcomes selected based on a combination of the player input with the corresponding input for each of the zero or more other participants.

Claim 25 is directed to an outcomes generator for verifiable gaming transactions comprising a commitment sequence executable to supply one or more players with a transformationally secured set of outcomes (see, e.g., Fig. 3, 351); and a reveal sequence responsive to receipt of transformationally secured player index contributions from each of the one or more players (see, e.g., 351 in Fig. 3), the reveal sequence executable to select a particular one of the outcomes based on a combination of the player indices.

Claim 28 is direct to a player client for verifiable gaming transactions comprising. An exemplary player client is shown in Figs. 2A and 2B and described on page 7, lines 11-22, paragraph 1024. The player include includes a commitment sequence executable, after receipt of a transformationally secured encoding of a predetermined set of outcomes (see e.g., 351 in Fig. 3), to supplying a transformationally secured encoding of a player input (see e.g., 352 in Fig. 3). The player includes a reveal sequence executable, after each of zero or more other participants in a gaming transaction has supplied a transformationally secured corresponding input, to reveal the player input (see, e.g. 354 in Fig. 3). A selector for a particular one of the outcomes is based on a combination of the player input with the corresponding input for each of the zero or more other participants.

Claim 29 is directed to a computer program product encoded in one or more computer readable media and comprising first instructions executable by a computing machine as part of a first commit/reveal protocol to supply one or more players with a transformationally secured set of outcomes (see, e.g., 351 in Fig. 3). The computer program product further includes second instructions executable by the computing machine to distribute transformationally secured player index contributions from each of the one or more players and only thereafter distribute the index contributions as part of a second commit/reveal protocol nested within the first commit/reveal protocol (see, e.g. 352, "SECURED X_i's, and 354 in Fig. 3). The computer program product further recites third instructions executable by the computing machine to reveal the set of outcomes (shown, e.g., 363 in Fig. 3).

Claim 31 is directed to a method of making a computer-readable encoding of a verifiable gaming outcome, the method comprising transformationally securing an encoding of a predetermined set of outcomes (see page 8, lines 1-4, paragraph 1026). The method further includes supplying one or more players with the transformationally secured encoding (see, e.g., 351 in Fig. 3). The method further includes receiving a transformationally secured player index from each of the one or more players (see, e.g., 352 in Fig. 3). The method further includes selecting a particular one of the outcomes for revealing to the one or more players based on a combination of the player indices (see, e.g. page 8, lines 5-11, paragraph 1027). The method also includes; encoding as the computer-readable encoding, information usable by the one or more players to reveal the selected outcome (see, e.g., page 10, lines 8-16, paragraph 1033).

Claim 35 is a means plus function claim. Claim 35 includes means for committing to a particular set of outcomes without revealing same. The means for committing to a particular set of outcomes without revealing the set of outcomes is illustrated in Figs. 1, 2A and 2B (outcomes/generator verifier 212, outcomes server 110C, outcomes generator/verifier 215). Fig. 1 illustrates an exemplary distributed gaming environment as described on page 6, lines 4-31, paragraphs 1020-1022. Figs. 2A and 2B are described on page 7, lines 1-26, paragraphs 1023 through 1025. Fig. 3 illustrates the means as the SHUFFLE (OPTIONAL) block and ENCRYPT block in Fig. 3 that supplies the encrypted deck 351. Page 8, lines 1-4, paragraph 1026 describe the game server 310 encrypting a possibly shuffled deck of cards and supplying an encoding 351 of the encrypted deck to all of the players. In that way the game server 310 commits to a particular (and possibly ordered) set of outcomes. The claim further recites means for ensuring an irrevocable commitment to respective index contributions by each party to a distributed transaction and only thereafter revealing a particular one of the outcomes based on a combination of the index contributions. Fig. 3 illustrates SECURED X_i's 352 being supplied from players 320 to gamer server 310 and the SECURED X_i's being forwarded from the game server 310 to the players 320. The game server then utilizes the X_i's 354 in computing a selected card. Pages 8, line 5 (paragraph 1027) through page 10, line 16 (paragraph 1033) describe various embodiments associated with the index contributions. Page 12, paragraph 1039 describes a particular computations model for dealing cards. Pages 13-14, paragraph 1043 also discusses index generation.

Claim 38 is directed to a method of facilitating verifiable gaming transactions in a distributed environment (see, e.g., Fig. 1), the method comprising committing a game server to a set of outcomes by supplying a transformationally secure encoding of the set of outcomes to one or more players (see, e.g., Fig. 3, 351); thereafter receiving from each player a commitment to a respective index contribution (352) and after receiving the commitment from each player, receiving from each player a communication revealing each respective index contribution (354); selecting from the set of outcomes based on a predefined combination operation on the index contributions (see, e.g., page 9, lines 6-13, paragraph 1030), and thereafter the game server revealing the set of outcomes for validation thereof (363).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Ground I: The rejection of claims 1-15, 17-38 under 35 U.S.C. § 102(e) as being anticipated by Schneier 6,099,408 (hereinafter Schneier).

Ground II: The rejection of claims 16 under 35 U.S.C. § 103(e) as being unpatentable over Schneier 6,099,408.

ARGUMENT

Ground I: The rejection of claims 1-15, 17-38 under 35 U.S.C. § 102(e) as being anticipated by Schneier 6,099,408 (hereinafter Schneier).

Claims 1-10

With respect to claim 1-10, applicants respectfully submit that Schneier fails to teach a nested first- and second-type commit reveal sequences having a first-type commit/reveal sequence that commits an outcome generator to a set of outcomes. In one embodiment of the invention a dealer (outcome generator) shuffles a deck of cards and commits to its order by communicating a secured encoding of deck order to the player. See page 2, paragraph 5 of the specification. Thus, in that particular embodiment, the set of outcomes committed to is deck order. The outcome generator may commit to other outcomes as described in the specification.

In Schneier, game server random numbers and player random numbers are used to define the card sequence. The Office Action maintains the claimed first commit sequence is taught by Schneier's combining the game server random numbers and players' random numbers to generate the card sequence. Applicants respectfully disagree that Schneier teaches committing an outcome generator to a set of outcomes. In Schneier, the game server cannot commit to a set of outcomes because the outcome is unknown when the game server supplies the players its random number and thus cannot teach the first-type commit reveal sequence. The Office action points to col. 13, lines 45 to col. 14, line 3 of Schneier to teach claim 1. However Schneier teaches at col. 13, lines 40-56:

> [I]n one embodiment of the invention, a result value represents the complete sequence of fifty-two cards. Once the card sequence is defined based on the player random number and the game server random number, the cards can be dealt.
>
> For example, after generating an encoded player random number and transmitting it to game server 200, player terminal 300 receives the encoded game server random number. Player terminal 300 then transmits a decoding key to game server 200 which generates the result value representing the complete sequence of cards in the deck. Before sending a game server decoding key to player terminal 300, game server 200 sends the player card values representing a hand of cards dealt from the sequence of cards generated by the result value. If he desires, the player then selects to draw additional cards for his blackjack hand, again, from the defined sequence of cards. [Emphasis added]

Claim 1 recites *that the first-type commit/reveal sequence commits an outcome generator to a set of outcomes*. Schneier teaches utilizing both player and game server random numbers to generate the deck order or card sequence. Schneier teaches that the player terminal sends an encoded random number. Then, the player terminal receives the encoded game server random number. Player terminal 300 then transmits a decoding key to game server 200 which generates the result value representing the complete sequence of cards in the deck. The encoded game server random number cannot commit the game server to a set of outcomes, because the player random number, which is decoded after sending the game server random number, is needed to determine the set of outcomes.

The reveal portion of the first-type commit/reveal sequence is recited in claim 1 as *thereafter revealing the set of outcomes for validation thereof.* The Office Action relies on Schneier supplying the game server decoding key at the end of the game to teach that limitation. However, the game server decoding key is not a set of outcomes. While the game server decoding key can be utilized with the player random numbers to validate the outcome, the game server decoding key does not reveal the set of outcomes to which the game server previously committed.

Anticipation under 35 U.S.C. § 102(e)(2) requires that the invention be described in a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent. 35 U.S.C. § 102 (2004). Anticipation requires that each and every element of the claimed invention be disclosed in a single prior art reference. Minnesota Mining & Mfg. Co. v. Johnson & Johnson Orthopaedics Inc., 976 F.2d 1559, 1556, 24 USPQ2d 1321, 1326 (Fed. Cir. 1992) (To establish anticipation a party "must show that each element of the claim in issue is found, either expressly or under principles of inherency, in a single prior art reference . . . ."). A prior art reference anticipates a claim only if the reference discloses, either expressly or inherently, every limitation of the claim. See also, Verdegaal Bros., Inc. v. Union Oil Co., 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "[A]bsence from the reference of any claimed element negates anticipation." Kloster Speedsteel AB v. Crucible, Inc., 793 F.2d 1565, 1571, 230 USPQ 81, 84 (Fed. Cir. 1986). As shown above, Schneier fails to teach each and every element of claim 1 and thus claim 1 and all claims dependent thereon are patentable over Schneier.

Claims 11-19

With regards to claim 11, the only independent claim of claim 11-19, applicants respectfully maintain that Schneier fails to teach *supplying one or more players with the transformationally secured encoding of a predetermined set of outcomes for a gaming transaction.* The Office Action maintains that Schneier teaches claim 11 all at column 13, lines 35 to col. 14, lines 18. However Schneier teaches at col. 13, lines 40-56:

> [I]n one embodiment of the invention, a result value represents the complete sequence of fifty-two cards. Once the card sequence is defined based on the player random number and the game server

> random number, the cards can be dealt.
>
> For example, after generating an encoded player random number and transmitting it to game server 200, player terminal 300 receives the encoded game server random number. Player terminal 300 then transmits a decoding key to game server 200 which generates the result value representing the complete sequence of cards in the deck. Before sending a game server decoding key to player terminal 300, game server 200 sends the player card values representing a hand of cards dealt from the sequence of cards generated by the result value. If he desires, the player then selects to draw additional cards for his blackjack hand, again, from the defined sequence of cards. [Emphasis added]

Schneier clearly teaches utilizing both player and game server random numbers to generate the deck order or card sequence. Schneier teaches that the player terminal sends an encoded random number. Then, the player terminal receives the encoded game server random number. Player terminal 300 then transmits a decoding key to game server 200 which generates the result value representing the complete sequence of cards in the deck. However, Schneier fails to teach *supplying one or more players with the transformationally secured encoding of a predetermined set of outcomes for a gaming transaction.* Applicants maintain that *the transformationally secured encoding* cannot be the encoded game server random number because the game server random number is not sufficient by itself to determine the predetermined set of outcomes. Thus, applicants maintain that Schneier fails to teach each and every limitation of claim 11 and that claim 11 and all claims dependent thereon distinguish over Schneier.

Claims 20-24

With regards to claim 20, applicants respectfully maintain that Schneier fails to teach *receiving a transformationally secured encoding of a predetermined set of outcomes for a gaming transaction.* The Office Action relies on Schneier col. 12, line 36 to col. 13, line 24. That portion of Schneier teaches that the game server transmits its encoded random number to the player terminals after the player terminals send their encoded random numbers. Game server 200 generates the game result after receiving the keys from the players. Thus, there is no teaching of receiving a transformationally secured encoding of a predetermined set of outcomes for a gaming transaction as required in claim 20. Neither the random numbers supplied by the

players nor by the game server is a transformationally secured encoding of a predetermined set of outcomes since both random numbers are required to determine the predetermined set of outcomes. Accordingly, applicants respectfully submit that claim 20 and all claims dependent thereon distinguish over Schneier for at least the reasons.

Claims 25-27

With regards to claim 25, applicants respectfully submit that Schneier fails to teach *a commitment sequence executable to supply one or more players with a transformationally secured set of outcomes*. As pointed out above, Schneier teaches supplying a game server random number but the game server random number is not used as a commitment sequence that supplies one or more players with a transformationally secured set of outcomes. The set of outcomes is not determined without both the game server and player random numbers. Accordingly, applicants respectfully submit that claim 25 and all claims dependent thereon distinguish over the references of record.

Claim 28

Applicants respectfully submit that Schneier fails to teach *a commitment sequence executable, after receipt of a transformationally secured encoding of a predetermined set of outcomes, to supplying a transformationally secured encoding of a player input*. The players in Schneier do supply an encoded player input but not in response to an encoded predetermined set of outcomes. The set of outcomes in Schneier is not determined without both the player and game server random numbers. The players in Schneier do receive an encoded game server random number but there is no receipt of a transformationally secured encoding of a predetermined set of outcomes since the game server random number is not sufficient to generate the outcomes. Thus, applicants respectfully submit that claim 28 distinguishes over the references of record for at least the reason given above.

Claims 29-30

With regards to claim 29 applicants respectfully submit that Schneier fails to teach first instructions executable as part of a first commit/reveal protocol to supply one or more players with a transformationally secured set of outcomes. As pointed out above, the random number

supplied by the game server does not describe a set of outcomes. Accordingly, applicants respectfully submit that claim 29 and all claims dependent thereon distinguish over the references of record for at least the reasons given above.

Claims 31-34

With regards to claim 31 applicants respectfully submit that Schneier fails to teach *transformationally securing an encoding of a predetermined set of outcomes and supplying one or more players with the transformationally secured encoding*. Nor does Schneier teach *selecting a particular one of the outcomes for revealing to the one or more players based on a combination of the player indices*. As pointed out above, Schneier fails to teach a transformationally secured encoding of a predetermined set of outcomes (such as deck order). Instead Schneier teaches that the game server transmits its encoded random number to the player terminals and the player terminals send their encoded random numbers to the game server. Game server 200 generates the game result after receiving the decoding keys from the players utilizing player and game server random numbers. Thus, Schneier cannot select a particular one of the predetermined set of outcomes supplied to the players because such outcomes were not supplied to the players. Accordingly, applicants respectfully submit that claim 31 and all claims dependent thereon distinguish over the references of record for at least the reason given above.

Claim 35

With regards to claim 35, applicants respectfully submit that Schneier fails to teach a *means for committing to a particular set of outcomes without revealing same*. That is disclosed in the specification as, e.g., the game server supplying an encoding of a shuffled deck to the players. Schneier teaches generating a game server random number that is utilized to determine the result along with player random numbers, but the game server random number does not by itself commit the game server to a particular set of outcomes such as deck order. Accordingly, applicants respectfully submit that claim 35 distinguishes over Schneier for at least the reasons given above.

Claims 36-37

Claims 36 and 37 recite that the set of outcomes correspond to deck order. Schneier cannot commit to deck order as the commit portion of a first commit/reveal sequence because the deck order is unknown when the game server sends its encoded random number to the players. Thus, claims 36 and 37 distinguish over Schneier.

Claim 38

Claim 38 recites *committing a game server to a set of outcomes by supplying a transformationally secure encoding of the set of outcomes to one or more players and thereafter receiving from each player a commitment to a respective index contribution and after receiving the commitment from each player, receiving from each player a communication revealing each respective index contribution; and selecting from the set of outcomes based on a predefined combination operation on the index contributions; and thereafter the game server revealing the set of outcomes for validation thereof.* Schneier does not teach committing the game server to a set of outcomes by supplying a transformationally secure encoding of the set of outcomes to one or more players and thereafter receiving from each player a commitment to a respective index contribution. Schneier instead teaches supplying an encoded game server random number to the player(s). See col. 13, lines 45-50. However, that gamer server random number does not commit the game server to an outcome because the outcome cannot be determined from the gamer server random number. Nor does Schneier teach the game server revealing the set of outcomes for validation. Schneier does teach the game server providing the decoded game server random number for validation but that is not the same as revealing the set of outcomes. Thus, for at least these reasons, applicants respectfully submit that claim 38 distinguishes over Schneier.

ARGUMENT

Ground II: The rejection of claims 16 under 35 U.S.C. § 103 as being unpatentable over Schneier 6,099,408.

Applicants respectfully submit that the failure of Schneier to teach elements of claim 11 as described above, renders claim 16 nonobvious over Schneier. The legal standard for obviousness is defined in the Patent Statute, 35 U.S.C. § 103:

> [a] patent may not be obtained though the invention is not identically disclosed or described [by prior art under 35 U.S.C. § 102] if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

35 U.S.C. § 103 (2004).

Obviousness is a legal determination based on underlying factual inquiries. Minnesota Min. & Mfg. Co. v. Johnson & Johnson Orthopedics, Inc., 976 F.2d 1559, 24 U.S.P.Q.2d 1321, 1332-1333 (Fed. Cir. 1992). Graham v. John Deere Co., 383 U.S. 1, 17 (1966) defines the factual inquiries utilized to evaluate the prior art. Specifically, the prior art is evaluated in terms of: (1) its scope and content; (2) the differences between the prior art and the claimed invention; (3) the level of ordinary skill in the art at the time the application was filed; and (4) objective, or secondary, evidence of nonobviousness such as commercial success, failure of others, long-felt need and unexpected results, which must be considered in reaching a conclusion of obviousness. Graham v. John Deere Co., 383 U.S. 1, 17, 148 U.S.P.Q. 459, 460 (1966); Panduit Corp. v. Dennison Mfg. Co., 810 F.2d 1561, 1566-67, 1 U.S.P.Q.2d 1593, 1595-96 (Fed. Cir. 1987); Minnesota Min. & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc., 976 F.2d 1559, 24 U.S.P.Q.2d 1321, 1333 (Fed. Cir. 1992). In the present appeal, the issue relates to specific differences between the prior art and appealed claim, specifically absence, in the relied upon reference, of key elements of the parent claim 11. All claim limitations must be considered in the obviousness analysis. Indeed, it is clear error to ignore limitations clearly set forth in the claims. Panduit Corp., 1 U.S.P.Q.2d, 1603 – 1604, 810 F.2d at 1576.

Schneier's failure to teach each and every element of claim 11 as described above, renders claim 16 nonobvious over Schneier.

CONCLUSION

For the at least the foregoing reasons, Appellants' respectfully submit that claims 1-38 distinguish over Schneier. Accordingly, the Board is respectfully requested to reverse the rejections of claims 1-38 and to direct the claims of the present application to be issued.

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that, on the date shown below, this correspondence is being

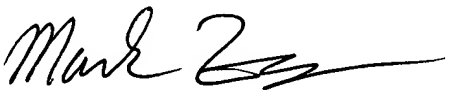
☐ deposited with the US Postal Service with sufficient postage as first class mail and addressed as shown above.

☐ facsimile transmitted to the US Patent and Trademark Office.

_____ _____
Date

EXPRESS MAIL LABEL: EV 671 081 865 US

Respectfully submitted,



Mark Zagorin, Reg. No. 36,067
Attorney for Applicant(s)
(512) 338-6311
(512) 338-6301 (fax)

CLAIMS APPENDIX

1. (Original) A method of facilitating verifiable gaming transactions in a distributed environment, the method comprising:

executing nested first- and second-type commit/reveal sequences, wherein the first-type commit/reveal sequence commits an outcome generator to a set of outcomes, and instances of the second-type commit/reveal sequence commit at least each player to a respective index contribution and only thereafter reveal the respective index contributions;

selecting from the set of outcomes based on a predefined combination operation on the index contributions; and

thereafter revealing the set of outcomes for validation thereof.

2. (Original) The method of claim 1,

wherein the set of outcomes correspond to card values from one or more decks thereof.

3. (Original) The method of claim 2,

wherein the cards values are shuffled.

4. (Original) The method of claim 2,

wherein the card values are unshuffled, but the predefined combination operation further operates on an index contribution of the outcome generator.

5. (Original) The method of claim 1, wherein the set of outcomes correspond to a set of values at least partially defined by one or more of:

a deck of cards;

sides of a die;

sides of a coin; and

slots of a wheel.

6. (Previously presented) The method of claim 1, wherein the first-type commit/reveal sequence includes:

encryption of the set of outcomes;

supply of the encrypted set of outcomes to each of the players; and

later access to the set of outcomes using a key.

7. (Original) The method of claim 1, wherein the first-type commit/reveal sequence includes:

encryption of individual ones of the outcomes;

supply of the ordered set of encrypted outcomes to each of the players; and

later access to the selected outcomes using respective keys.

8. (Original) The method of claim 1, wherein the second-type commit/reveal sequence includes:

hashing of respective index contribution using a predetermined hash;

supply of the hashed index contributions to the outcome generator and to all of the players; and

later supply of the index contributions to the outcome generator and to all of the players.

9. (Original) The method of claim 1,

wherein the first- and second-type commit/reveal sequences include respective transformational securings selected from the set of cryptographic encodings, hashes and irreversible transforms.

10. (Original) The method of claim 1,

wherein the first-type commit/reveal sequence is performed substantially by a game processor; and

wherein the second-type commit/reveal sequence is performed substantially by respective player processors.

11. (Original) A verifiable gaming transactions method comprising:

transformationally securing an encoding of a predetermined set of outcomes;

supplying one or more players with the transformationally secured encoding;

receiving a transformationally secured player index from each of the one or more players; and

selecting a particular one of the outcomes for revealing to the one or more players based on a combination of the player indices.

12. (Original) The method of claim 11,

wherein the predetermined set of outcomes is transformationally secured using a cryptographic key; and

wherein the player indices are transformationally secured using a hash.

13. (Original) The method of claim 11, further comprising:

receiving and verifying the player indices against respective transformationally secured player indices prior to the outcome selecting.

14. (Original) The method of claim 11, further comprising:

randomizing ordering of the predetermined set of outcomes prior to the securing thereof.

15. (Previously Presented) The method of claim 11, further comprising:

effectively randomizing the set of outcomes by further combining the player indices with a randomized index.

16. (Original) The method of claim 11,

wherein the combination includes a bit-wise exclusive OR of binary encodings of the player indices.

17. (Original) The method of claim 11,

wherein the selecting includes a modulo function.

18. (Previously Presented) The method of claim 11,

wherein the transformational securing of the predetermined set of outcomes includes cryptographically securing the set of outcomes.

19. (Previously Presented) The method of claim 11,
wherein the transformational securing of the predetermined set of outcomes includes cryptographically securing individual outcomes of the set thereof.

20. (Original) A verifiable gaming transactions method comprising:
receiving a transformationally secured encoding of a predetermined set of outcomes for a gaming transaction;
supplying a transformationally secured encoding of a player input;
after each of zero or more other participants in the gaming transaction has supplied a transformationally secured corresponding input, supplying the player input; and
accessing a particular one of the outcomes selected based on a combination of the player input with the corresponding input for each of the zero or more other participants.

21. (Original) The method of claim 20, further comprising:
supplying successive player inputs after prior supply and receipt of corresponding transformationally secured inputs; and
accessing successive one of the outcomes selected based on combination of the successively supplied player inputs with the corresponding inputs for each of the zero or more other participants.

22. (Original) The method of claim 20,
wherein the accessing includes receiving an encoding of the particular outcome subject to later verification against the transformationally secured set of outcomes.

23. (Original) The method of claim 20,
wherein outcomes of the transformationally secured set thereof are individually secured; and
wherein the accessing includes obtaining a key for a corresponding individually secured outcome.

24. (Previously Presented) The method of claim 20,

wherein outcomes of the transformationally secured set thereof are individually secured; and

wherein the accessing includes receiving an encoding of the particular outcome for verification against corresponding individually secured outcome.

25. (Original) An outcomes generator for verifiable gaming transactions comprising:

a commitment sequence executable to supply one or more players with a transformationally secured set of outcomes; and

a reveal sequence responsive to receipt of transformationally secured player index contributions from each of the one or more players, the reveal sequence executable to select a particular one of the outcomes based on a combination of the player indices.

26. (Original) The outcomes generator of claim 25,

integrated with, and responsive to, game logic.

27. (Original) The outcomes generator of claim 25,

wherein the commitment and reveal sequences employ cryptographic transformations.

28. (Original) A player client for verifiable gaming transactions comprising:

a commitment sequence executable, after receipt of a transformationally secured encoding of a predetermined set of outcomes, to supplying a transformationally secured encoding of a player input; and

a reveal sequence executable, after each of zero or more other participants in a gaming transaction has supplied a transformationally secured corresponding input, to reveal the player input; and

a selector for a particular one of the outcomes based on a combination of the player input with the corresponding input for each of the zero or more other participants.

29. (Original) A computer program product encoded in one or more computer readable media and comprising:

first instructions executable by a computing machine as part of a first commit/reveal protocol to supply one or more players with a transformationally secured set of outcomes;

second instructions executable by the computing machine to distribute transformationally secured player index contributions from each of the one or more players and only thereafter distribute the index contributions as part of a second commit/reveal protocol nested within the first commit/reveal protocol; and

third instructions executable by the computing machine to reveal the set of outcomes.

30. (Original) The computer program product of claim 29,

wherein the one or more computer readable media are selected from the set of a disk, tape or other magnetic, optical, or electronic storage medium and a network, wireline, wireless or other communications medium.

31. (Original) A method of making a computer-readable encoding of a verifiable gaming outcome, the method comprising:

transformationally securing an encoding of a predetermined set of outcomes;

supplying one or more players with the transformationally secured encoding;

receiving a transformationally secured player index from each of the one or more players;

selecting a particular one of the outcomes for revealing to the one or more players based on a combination of the player indices; and

encoding as the computer-readable encoding, information usable by the one or more players to reveal the selected outcome.

32. (Previously Presented) The method of claim 31,

wherein the information encodes the selected outcome.

33. (Previously Presented) The method of claim 31,

wherein the information includes a key to reveal at least the selected one of the outcomes from the supplied transformationally secured encoding thereof.

34. (Previously Presented) The method of claim 31,

wherein the computer-readable encoding includes at least one message suitable for communication between a gaming server and a client thereof.

35. (Original) An apparatus comprising:

means for committing to a particular set of outcomes without revealing same; and

means for ensuring an irrevocable commitment to respective index contributions by each party to a distributed transaction and only thereafter revealing a particular one of the outcomes based on a combination of the index contributions.

36. (Previously Presented) The method of claim 1,

wherein the set of outcomes corresponds to deck order.

37. (Previously Presented) The method of claim 11,

wherein the predetermined set of outcomes corresponds to deck order.

38. (Previously Presented) A method of facilitating verifiable gaming transactions in a distributed environment, the method comprising:

committing a game server to a set of outcomes by supplying a transformationally secure encoding of the set of outcomes to one or more players;

thereafter receiving from each player a commitment to a respective index contribution and after receiving the commitment from each player, receiving from each player a communication revealing each respective index contribution;

selecting from the set of outcomes based on a predefined combination operation on the index contributions; and

thereafter the game server revealing the set of outcomes for validation thereof.

EVIDENCE APPENDIX

There is no evidence submitted pursuant to 37 C.F.R. § 1.130, 1.131, or 1.132 or any other evidence entered by the examiner and relied upon by appellant in the appeal.

RELATED APPEALS APPENDIX

There are no decisions rendered by a court or the Board in any proceeding identified above in the Related Appeals and Interferences section.